F O R E W O R D

1. This Network Management (NM) military handbook is approved for use by all Departments and Agencies of the U.S. Department of Defense (DoD).

2. Beneficial comments (recommendation, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to:

Joint Interoperability and Engineering Organization
Attn: JIEO-TBBD
Fort Monmouth, New Jersey 07703-5613

by using the self-addresses Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

3. This document is a product of collective efforts of the MILDEPs through the DoD Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) NM Working Group (WG 4) and the National Institute of Standards and Technology (NIST).

CONTENTS

LIST OF FIGURES

NUMBER PAGE

1. SCOPE

1.1 Scope. Military Handbook (MIL-HDBK) 2045-38000 defines network management (NM) requirements for DoD communications systems. This MIL-HDBK is targeted for manager systems as well as all logical and physical communications resources and systems to be managed. Over time this MIL-HDBK will evolve and be targeted for the management of all distributed information processing resources in a networked environment (see Appendix C). This MIL-HDBK complements and provides guidance for the DoD's implementation of the *Government Network Management Profile*(GNMP) Phase I. It will evolve concurrently with the GNMP.

The GNMP is intended to be a complete profile, specifying all that is necessary to assure that a NM system product procured in accordance with its specifications will interoperate with any other NM system product procured in accordance with the GNMP and provide services generally useful for network administrators. These services include NM information retrieval and control. They do not include services such as NM information analysis, display and decision-making.

This MIL-HDBK provides an added level of detail that includes selected requirements and functionality that transcend the basic management protocol interoperability addressed by GNMP. Examples of these areas are the human-machine interface, automated analysis, NM system database characteristics and performance requirements. Many such requirements are acquisition-specific and the quantification of such requirements into testable procurement requirements will be the responsibility of the Cognizant Technical Official (CTO). Still other areas, such as power requirements, physical plant facilities, acceptance testing requirements, etc., are also acquisition-specific and go beyond the scope of this document.

1.2 Purpose. The purpose of this military handbook for NM is:

a. to be the evolving repository for descriptions of unique NM requirements applicable to DoD;

b. to provide guidance for the procurement of interoperable NM products and services for DoD communications systems;

c. to direct that Open Systems Interconnection (OSI)-based management, as represented in the GNMP, is DoD's strategic management solution;

d. to indicate that a number of relevant *de jure* and *de facto* (governmental/national/ international and industry) standards and implementation agreements can be referenced in DoD procurement of NM products and services;

e. to assist in the procurement of standards-based, conformant, commercial off-the-shelf (COTS) NM products and services whenever possible in order to avoid excessive development time and life cycle costs typically associated with proprietary NM products and services;

f. to stress DoD's near-term commitment to begin procuring NM products and services that, at a minimum, conform to GNMP for basic interoperability among distributed, heterogeneous NM products and services;

g. to identify high-level requirements (in areas that go beyond the scope of GNMP) that must be considered by CTOs and, as needed, should be translated by specific CTOs into acquisition-specific, testable requirements; and

h. to alert DoD personnel involved with networks, systems and networking that management functions, capabilities and activities associated with such resources should be considered throughout the life cycle of such resources, from early planning stages, throughout daily operation and growth, to the end of retirement.

1.3 Applicability. This MIL-HDBK augments the GNMP with DoD-specific requirements. In particular, this MIL-HDBK provides guidance for:

a. the acquisition of analog and digital networks, communication resources and/or communication services; and

b. the acquisition of accompanying management systems and/or management system components, capabilities or services for such networks, resources and services.

This MIL-HDBK provides for multiple vendor network/communications capabilities acquired by one procurement to be manageable by other vendors' manager systems acquired by another procurement. The application of this MIL-HDBK to the acquisition of other new systems, such as end systems (e.g., computers) that use network and/or communications products/services, or to the retrofitting of, or interfaces to, existing systems is to be determined on a case-by-case basis by the CTO.

The development of standards-based Voice Oriented Telecommunications Network Management Systems (VOT NMSs) is just beginning. Consequently, this MIL-HDBK acknowledges that VOT NMS products that conform to this MIL-HDBK may not be available. As this MIL-HDBK evolves, it will be expanded to cover products and services of the VOT NMS as they mature.

1.4 Limitations. By using this MIL-HDBK throughout the DoD, it will be possible to have multiple vendor network/communications capabilities acquired by one procurement be manageable by other vendors' manager systems acquired by another procurement. However, it should be noted that not all aspects of interoperability pertinent to NM have reached the level of maturity and preciseness as those aspects specified in the GNMP. In those areas for which implementation profiles such as those specified in the GNMP do not yet exist, full interoperability across NM elements procured under different acquisition is at risk. This is especially true for acquisitions based on those references lower in the order of alternative sources of specifications in section 1.9 of this MIL-HDBK. SNMP-based COTS solutions will be much more widely available than CMIS-CMIP solutions and can be used to fulfill requirements that are not yet met by rigorous, stable, industry-accepted implementation profiles. However careful consideration must be given to provide the best present

solution while at the same time providing a migration path to a fully interoperable open NM system. See section 1.9.1.

1.5 Relationship to the GNMP. The GNMP, the Federal Information Processing Standard (FIPS 179) for NM, is the standard for all Federal Government agencies to use when acquiring NM products, functions and services for computer and communications systems and networks. The GNMP provides implementation specifications for the Common Management Information Services and Protocol (CMIS/CMIP), specific management functions and services, and the syntax and semantics of the management information required to support monitoring and control of logical and physical resources associated with network and system components.

This MIL-HDBK will build upon the GNMP by describing common military architectures and requirements, and manageable computer and communications resources. To address current, basic, OSI-oriented, NM interoperability requirements, implementors should consult this MIL-HDBK. In addition, if the DoD identifies general NM interoperability requirements which are not addressed in the GNMP, efforts shall be made to include them in future editions of the GNMP. Additional management capabilities and managed objects will be included in subsequent releases of the GNMP. To address other requirements, implementors should consult the other sources of specifications identified in Section 1.9.

1.6 Relationship to the Government Open Systems Interconnection Profile (GOSIP). The GOSIP (FIPS Pub 146-1) defines a common set of data communication protocols that enable systems developed by different vendors to interoperate enabling users of different applications on those systems to exchange information. The GOSIP also specifies services, such as File Transfer, Access and Management (FTAM), Message Handling Systems (MHS), and Virtual Terminal (VT), that can be used to support NM applications. In accordance with the GNMP, NM systems products and services should meet applicable requirements of the FIPS Pub 146-1.

It is expected that future versions of this MIL-HDBK will use other future GOSIP application services, such as Remote Database Access (RDA), Electronic Data Interchange (EDI), and Transaction Processing (TP), to support future NM applications. It should be noted that it is expected that future versions of the GOSIP FIPS will reference specifications in a new, more-encompassing initiative called IGOSS (Industry/Government Open Systems Specifications). IGOSS, under joint development by the Electric Power Industry, the Manufacturing Automation Protocol and Technical Office Protocol (MAP/TOP) initiatives, and NIST, is scheduled for promulgation in early 1994.

1.7 Relationship to the OMNI*Points*. OMNI*Point* specifications are profiles of specifications that foster common management functionality and portability, as well as interoperability among heterogeneous management components. OMNI*Points* are defined in the Open Management Roadmap, an international partnership of government, industry, vendors, and users. OMNI*Point* 1, a set of intercept points for standards and implementations, is summarized in Appendix D.

The Open Management Roadmap, initiated and managed by the Network Management Forum (NMF), is an endeavor to coordinate all the related activities needed to develop

comprehensive, open, turn-key enterprise management solutions. These activities include developing standards, defining implementation specifications, and defining and conducting interoperability and conformance tests for the many technical aspects of turn-key, enterprise management solutions. These specifications and testing services are bundled into OMNI*Points*, which are released bi-annually. Such OMNI*Points* allow vendors and users to build and to buy distributed, portable, evolvable and interoperable NM products and services, as well as general purpose management platforms, such as those that employ the Distributed Management Environment (DME) technology of the Open Software Foundation (OSF). Such platforms can host other OMNI*Point* products and services, such as NM applications software. The GNMP is an integral part of the first OMNI*Point* specification.

1.8 Relationship to the Simple Network Management Protocol (SNMP). SNMP is a part of the first OMNI*Point.* It is the current industry *de facto* standard for managing a growing set of resources primarily within TCP/IP-based networks, e.g., routers, as well as a growing set of resources that are interconnected by such networks and the multiple vendor pool of protocol analyzers used to assist NM personnel. SNMP currently plays a major role in the management of military and civilian communications resources.

SNMP and SMNP v2 are standards developed by the Internet Engineering Task Force (IETF), an organization of vendors/users who implement the DoD TCP/IP protocol suite. Activities of the IETF are overseen by the Internet Advisory Board (IAB) and its parent organization, the Internet Society (ISOC). Each Internet standard is documented in a numbered Request for Comment (RFC); for example, SNMP is documented in RFC 1157.

Although the intent of this MIL-HDBK is to support the acquisition of NM products and services that conform to OSI NM standards, it does not preclude the acquisition of specific COTS products and services that are based on use of industry standards such as SNMP and its potential successors, e.g., the Simple Network Management Protocol v2 (SNMP v2), in situations where OSI network management products have not yet been developed. SNMP is expected to have utility and be cost-effective for the management of certain non-OSI resources for the foreseeable future.

1.9 Sources of Specifications. When CTOs intend to procure NM products and services that incorporate management functions, services, protocols and information that are equivalent to that specified in the GNMP, the GNMP must be used as the source of implementation specifications for such procurement.

The GNMP does not address all the requirements in this MIL-HDBK. When CTOs intend to procure NM products and services that meet those requirements in this MIL-HDBK that are not addressed by the GNMP, then the CTOs (1) should use the other sources of specifications identified below, and (2) should use them in the order specified below:

a. if the specific requirements are addressed by other OMNI*Point* 1 specifications, then these OMNI*Point* 1 specifications should be used; otherwise,

b. if the specific requirements are addressed by current versions of the Open Systems Environment (OSE) Working Implementation Agreements, then these Agreements should be used; otherwise,

c. if the specific requirements are addressed by current preliminary versions of national/international standards, then these standards should be used; otherwise,

d. if the specific requirements are addressed by documents developed by specific consortia, then these documents should be used.

1.9.1 Transition Considerations. The CTO should ensure that future NM systems comply with the GNMP and/or OMNIPoints whenever possible. Throughout the initial period of the application of this handbook, many existing SNMP-based and legacy systems will still exist. They should not be replaced as long as they are operationally and economically viable. Integrating future NM systems with them should be carefully evaluated to prevent costly software upgrades to proprietary systems. A transition plan should be developed to determine how these existing systems will be integrated, upgraded, or phased out. Transition to a fully interoperable, open system is a prime consideration when deciding whether to integrate new and existing systems.

1.10 Appendices. This MIL-HDBK is supplemented by a number of appendices which will provide additional guidance and information.

a. Development of military-unique managed objects. Appendix A describes a general process for the definition of technical requirements for the management of military systems and resources to be managed in an integrated fashion using OSI NM techniques.

b. Additional considerations. Appendix B describes additional requirements for NM system facilities to support NCC managers at DoD sites, telecommunications managers, and data communications managers.

c. Distributed information processing environment within future scope of MIL-HDBK - 1351. Appendix C describes how the major classes of manageable resources within many types of organizations can be classified into groups or domains. Such classes of resources can be expected to be included in future versions of MIL-STD 2045-38000.

d. Overview of OMNI*Point* specifications. Appendix D describes the OMNI*Point* specifications which are profiles of specifications that foster common management functionality and portability, as well as interoperability among heterogeneous management components.

e. ISO NM-related standards. Appendix E gives a brief overview of ISO NM-related standards. This overview will help interested parties determine whether or not the ISO standards need to be consulted.

f. NATO Systems Management. Appendix F gives a brief overview of systems management within the NATO arena.

g. Security Threats and Mechanisms. Appendix G gives a brief overview of 5 of the principle threats to NM security and 7 security mechanisms.

h. Relationships Between Security Domains and Management Domains. Appendix H gives a brief definition of a security domain and a management domain and presents an illustrative representation of their possible relationships.

i. General Security Management Principles and Requirements. Appendix I lists some principles which may be applied for a security management system.

j. Information Reference Model for DoD NM Systems. Appendix J stresses the importance of developing a single perspective of DoD communications domains in order to highlight differences which exist within NM systems.

2. APPLICABLE DOCUMENTS

2.1 Government documents. Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from the Documents Order Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.

2.1.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the *Department of Defense Index of Specifications and Standards (DODISS)* and supplement thereto, cited in the solicitation (see section 6.2).

2.1.1.1 Specifications. Military SND.401 - *Secure Data Network Systems (SDNS) Security Protocol 4 (SP4)*, Revision 1.3, National Security Agency.

2.1.1.2 Federal Government and DoD standards. Relevant Federal Government and DoD standards include:

a. FIPS Pub 179, *Government Network Management Profile (GNMP)* 15 Dec 92.

b. FIPS Pub 146-1, *Government Open Systems Interconnection Profile (GOSIP)* version 2.0, 3 Apr 91.

c. *Industry/Government Open Systems Specifications (IGOSS)*- Version 1 Draft, Jan 93.

d. FED-STD-1037, *Glossary of Telecommunication Terms*

e. DOD 5200.28-STD, *DoD Trusted Computer System Evaluation Criteria*

f. MIL-STD-2204, *Survivable Adaptable Fiber Optic Embedded Network (SAFENET)*

g. N/SP-STD-1100B (Draft), *Interface Protocol Engineering Standard for the North American Aerospace Defense Command and the United States Space Command*

h. NISTIR 4792, *A Formal Description of the SDNS Security Protocol at Layer 4 (SP4)* Wayne Jansen, Mar 92.

2.1.2 Other government documents, drawings, and publications. The following government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

2.1.2.1 National Institute of Standards and Technology (NIST). Copies of NIST documents may be obtained from: National Technical Information Services (NTIS), U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161. Relevant NIST documents include:

a. NIST Special Publication 500-175, *Management of Networks Based on Open Systems Interconnection (OSI) Standards: Functional Requirements and Analysis*, Nov 89.

b. NIST Special Publication 500-206, *Stable Implementation Agreements for Open Systems Interconnection Protocols*, Open Systems Environment Implementors' Workshop, Version 6, Edition 1, Dec 92 (N.B., updated quarterly).

c. *Working Implementation Agreements for Open Systems Interconnection Protocols*, Open Systems Environment Implementors' Workshop, issued 21 Sep 92 (N.B., updated quarterly).

2.1.2.2 Defense Information System Agency (DISA). Copies of DISA documents may be obtained from DISA/JIEO, Attn: TBD, 11440 Isaac Newton Square, Reston, VA 22090. (NOTE: TBD is a DISA office symbol, not "to be determined") Relevant DISA documents include:

a. *Technical Reference Model for Information Management*, Defense Information Systems Agency, Center for Information Management, version 2.0, coordination draft, 22 Jun 93.

b. *Joint Communications Network Planning and Management System: Objective System Characteristics and Implementation Plan*, Final Report, TR 92-12-A, 30 Sep 92. (N.B., use office symbol *TFDX* instead of *TBD* for this document.)

c. *Defense Information Systems Network: A Goal Integrated Communications Architecture and Transition Strategy*, Final Report, Aug 92.

d. *Human-Computer Interface Style Guide*, Defense Information Systems Agency, Center for Information Management, version 2.0, 30 Sep 92.

2.1.2.3 North Atlantic Treaty Organization (NATO). Copies of NATO documents may be obtained from DISA (address to be determined). Relevant NATO documents include:

a. STANAG 4250-4, *NATO Reference Model for Open Systems Interconnection, Part 4, Management*, (Draft).

b. STANAG 4407, *NATO Reference Model for Open Systems Interconnection, Systems Management*, (Draft).

2.1.2.4 U.S. Army Information Systems Command (USAISC). Copies of USAISC documents may be obtained from USAISC, ASQB-OSI-S, Fort Huachuca, AZ 85613-5300. Relevant USAISC documents include *Network and Systems Management Functional Definition*, R. F. Moller, J. H. Rutter, and B. Zielinski, August 1992.

2.2 Non-government publications. The following documents form a part of this handbook to the extent specified herein. Unless otherwise specified, the issues of these DoD-adopted documents are those listed in the issue of the DODISS cited in the solicitation. Unless otherwise specified, the issues of documents not listed in the DODISS are the issues of the documents cited in the solicitation.

2.2.1 International Organization for Standardization/International Electrotechnical Committee (ISO/IEC), International Telegraph and Telephone Consultative Committee (CCITT) and Institute of Electrical and Electronics Engineers (IEEE) publications. Relevant documents from these standards bodies are as listed in the GNMP and in the GOSIP. Other relevant documents are listed below. Copies of ISO/IEC and CCITT documents may be obtained from: American National Standards Institute (ANSI), Attn: Sales Department, 11 West 42nd Street, New York, NY 10036. Copies of IEEE documents may be obtained from: IEEE, Inc., 345 East 47th Street, New York, NY 10017-2394.

a. CCITT Recommendation X.500, Information Technology - Opens Systems Interconnection - The Directory: Overview of Concepts, Models, and Services, Draft April 1992.

b. International Standard 7498-2 (ISO), Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, version 1, February 1989.

c. Information technology - Open Systems Interconnection -Generic Upper Layer Security - Part 1: Overview, Models, and Notation, CCITT Draft Rec.X.guls, ISO/IEC 11586-1.

d. Information technology - Open Systems Interconnection -Generic Upper Layer Security - Part 2: Security Exchange Service Element (SESE) Service Definition, CCITT Draft Rec.X.guls, ISO/IEC 11586-2.

e. Information technology - Open Systems Interconnection - Generic Upper Layer Security - Part 3: Security Exchange Service Element (SESE) Protocol Specification, CCITT Draft Rec.X.guls, ISO/IEC 11586-3.

f. Information technology - Open Systems Interconnection - Generic Upper Layer Security - Part 4: Generic Protecting Transfer Syntax, CCITT Draft Rec.X.guls, ISO/IEC 11586-4.

g. Information technology- Open Systems Interconnection - Systems Management - Part 8: Security Audit Trail Function, CCITT Rec. X.7xx, ISO/IEC IS 10164-8, 01992.

h. Information technology- Open Systems Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control, CCITT Rec. X.740, ISO/IEC 10164-9.

i. Information technology- Open Systems Interconnection - Systems Management - Part 10: Accounting Meter Function, CCITT Rec. X.7yy, ISO/IEC 10164-10.

j. Information technology- Open Systems Interconnection - Systems Management - Part 11: Metric Objects and Attributes, CCITT Rec. X.739, ISO/IEC 10164-11.

k. Information technology- Open Systems Interconnection - Systems Management - Part 12: Test Management Function, CCITT Rec. X.745, ISO/IEC 10164-12.

l. Information technology- Open Systems Interconnection - Systems Management - Part 13: Summarization Function, CCITT Rec. X.738, ISO/IEC 10164-13.

m. Information technology- Open Systems Interconnection - Systems Management - Part 14: Confidence and Diagnostic Test Categories, CCITT Rec. X.737, ISO/IEC 10164-14.

n. Information technology- Open Systems Interconnection - Systems Management - Part 15: Scheduling Function, CCITT Rec. X.746, ISO/IEC 10164-15.

o. Information technology- Open Systems Interconnection - Systems Management - Part 16: Management Knowledge Management Function, CCITT Rec. X.750, ISO/IEC 10164-16.

p. Information technology- Open Systems Interconnection - Systems Management - Part x: General Relationship Management Function, CCITT Rec. X.7yy, ISO/IEC 10164-x.

q. Information technology- Open Systems Interconnection - Systems Management - Part x: Software Management Function, CCITT Rec. X.7yy, ISO/IEC 10164-x.

r. Information technology- Open Systems Interconnection - Systems Management - Part x: Time Management Function, CCITT Rec. X.7yy, ISO/IEC 10164-x.

s. Information technology- Open Systems Interconnection - Systems Management - Part x: Response Time Monitoring Function, CCITT Rec. X.7yy, ISO/IEC 10164-x.

t. Information technology- Open Systems Interconnection - Systems Management - Part x: Change Over Function, CCITT Rec. X.7yy, ISO/IEC 10164-x.

u. Information technology- Open Systems Interconnection - Systems Management - Part x: Management Domain Management Function, CCITT Rec. X.7yy, ISO/IEC 10164-x.

v. Information technology- Open Systems Interconnection - Systems Management - Part x: Enhanced Event Handling and Log Control, CCITT Rec. X.7yy, ISO/IEC 10164-x.

w. Information technology- Open Systems Interconnection - Management Information Services - Structure of Management Information - Part 5: Generic Management Information, CCITT Rec. X.723, ISO/IEC 10165-5.

x. Information technology- Open Systems Interconnection - Management Information Services - Structure of Management Information - Part 6: Guidelines for Conformance Statement Proforma, CCITT Rec. X.724, ISO/IEC 10165-6.

y. Information technology- Open Systems Interconnection - Management Information Services - Structure of Management Information - Part x: Application Context for Systems Management with Transaction Processing, CCITT Rec. X.7yy, ISO/IEC 10165-x.

z. Information technology- Open Systems Interconnection - Management Information Services - Structure of Management Information - Part x: General Relationship Model, CCITT Rec. X.7yy, ISO/IEC 10165-x.

aa. ISO/CCITT and Internet Management Coexistence (IIMC): Translation of Internet MIBs to ISO/CCITT GDMO MIBs. (Also to be available as Internet Informational RFC.)

bb. ISO/CCITT and Internet Management Coexistence (IIMC): Translation of Internet MIB-II (RFC1213) to ISO/CCITT GDMO MIB. (Also to be available as Internet Informational RFC.)

cc. ISO/CCITT and Internet Management Coexistence (IIMC): ISO/CCITT to Internet Management Proxy. (Also to be available as Internet Informational RFC.)

dd. ISO/CCITT and Internet Management Coexistence (IIMC): ISO/CCITT to Internet Management Security. (Also to be available as Internet Informational RFC.)

ee. ISO/CCITT and Internet Management Coexistence (IIMC): Translation of ISO/CCITT GDMO MIBs to Internet MIBs. (Also to be available as Internet Informational RFC.)

2.2.2 Internet Engineering Task Force (IETF) publications. Information on the IETF activities can be obtained from: Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA 22091. RFCs may be obtained electronically through various means.

a. RFC 1155 - *Structure and Identification of Management Information (SMI) for TCP/IP-based Internets*, May 1990.

b. RFC 1157 - *A Simple Network Management Protocol (SNMP)* May 1990.

c. RFC 1213 - *Management Information Base (MIB-II) for Network Management of TCP/IP-based Internets*, March 1991.

d. RFC 1351 - *SNMP Administrative Model*, July 1992.

e. RFC 1352 - *SNMP Security Protocols*, July 1992.

f. RFC 1353 - *Definitions of Managed Objects for Administration of SNMP Parties*, July 1992.

2.2.3 Industry standards.

a. The OMNI*Point* 1 specifications are available from: Network Management Forum, 40 Morristown Rd, Bernardsville, NJ 07924. Tel: (908) 766-1544.

b. The IGOSS specifications are available from: Standards Office, National Institute of Standards and Technology, building 225, Room B64, Gaithersburg, MD 20899. Tel: (301) 975-2816.

2.2.4 Regional Workshop Coordinating Committee (RWS-CC) Technical Reports (TRs). RWS-CC TRs may be obtained from the European Workshop for Open Systems, Rue de Stassart 36, 7th Fl., B-1050 Brussels Belgium, Tel: +32-2-511-74-55.

a. Framework for Conformance and Testing of OSI System Management Profiles.

b. Managed Object Conformance Testing Methodology.

2.2.5 OSInet Publications. OSInet Network Management Interoperability Test Suites publications may be obtained from OSInet c/o Corp for Open Systems International, 1750 Old Meadow Rd., McLean VA 22102, Tel (703)-205-2750.

2.3 Order of precedence. In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 Acronyms. The acronyms used in this handbook are defined as follows:

ACSE	-	Association Control Service Element
AE	-	Application Entity
AM	-	Accounting Management
ANSI	-	American National Standards Institute
API	-	Application Programming Interface
ASN.1	-	Abstract Syntax Notation One
CCITT	-	International Telegraph and Telephone Consultive Committee
CLNP	-	Connectionless Network Protocol
CLNS	-	Connectionless Network Service
CMIP	-	Common Management Information Protocol
CMIS	-	Common Management Information Services
CM	-	Configuration Management
COMSEC	-	Communications Security
CONOPS	-	Concept of Operations
CONS	-	Connection-Oriented Network Service
CONUS	-	Continental United States
CORBA	-	Common Object Request Broker Architecture
COTS	-	Commercial Off-the-Shelf
CSMA/CD	-	Carrier Sense Multiple Access/Collision Detection
CTO	-	Cognizant Technical Official
DAA	-	Designated Accreditation Authority
DACS	-	Digital Access and Cross-connect System
DBMS	-	Database Management System
DCE	-	Distributed Communication Environment
DCPS	-	Data Communications Protocol Standards
DDN	-	Defense Data Network
DES	-	Data Encryption Standard
DISA	-	Defense Information Systems Agency (DoD)
DISN	-	Defense Information Systems Network
DISP	-	Draft International Standardized Profile (ISO)
DME	-	Distributed Management Environment (OSF)
DMS	-	Defense Message System
DoD	-	Department of Defense
DODISS	-	DoD Index of Specifications and Standards
DPAS	-	Digital Patch and Access System
DSN	-	Defense Switched Network
DTE	-	Data Terminal Equipment
DTMP	-	DCPS Technical Management Panel (DoD)
EDI	-	Electronic Data Interchange

E-mail	-	Electronic mail
FDDI	-	Fiber Distributed Data Interface
FIPS	-	Federal Information Processing Standard
FM	-	Fault Management
FTAM	-	File Transfer, Access and Management
GDMO	-	Guidelines for the Definition of Managed Objects
GNMP	-	Government Network Management Profile
GOSIP	-	Government Open Systems Interconnection Profile
HMI	-	Human-Machine Interface
IAB	-	Internet Advisory Board
IEEE	-	Institute of Electrical and Electronics Engineers
IETF	-	Internet Engineering Task Force
IFIP	-	International Federation of Information Processing
IGOSS	-	Industry/Government Open Systems Specification
ISDN	-	Integrated Services Digital Network
ISO	-	International Organization for Standardization
ISOC	-	Internet Society
ISP	-	International Standardized Profile
ISYSCON	-	Integrated System Control (U.S. Army)
KDC	-	Key Distribution Center
LAN	-	Local Area Network
LLC	-	Logical Link Control Protocol
MAC	-	Media Access Control
MAN	-	Metropolitan Area Network
MAP	-	Manufacturing Automation Protocol
MHS	-	Message Handling System
MILDEP	-	Military Department
MIB	-	Management Information Base
MIB-II	-	the current implementation of the Internet MIB
MIL-STD	-	Military Standard
MLS	-	Multi-Level Security
MTBF	-	Mean Time Between Failure
MTTF	-	Mean Time To Failure
MTTR	-	Mean Time To Repair
NACISA	-	NATO Communications and Information Systems Agency
NATO	-	North Atlantic Treaty Organization
NCC	-	Network Control Center
NE	-	Network Element
NIST	-	National Institute of Standards and Technology
NM	-	Network Management
NMF	-	Network Management Forum
NTIS	-	National Technical Information Services
OIW	-	OSE Implementors' Workshop
OMG	-	Object Management Group

OODMBS	-	Object-Oriented DBMS
OSE	-	Open Systems Environment
OSF	-	Open Software Foundation
OSI	-	Open Systems Interconnection
PBX/PABX	-	Private (Automated) Branch Exchange
PDU	-	Protocol Data Unit
PM	-	Performance Management
PSAP	-	Presentation Service Access Point
RDBMS	-	Relational DBMS
RDA	-	Remote Database Access
RFC	-	Request for Comment (IETF)
RPC	-	Remote Procedure Call
ROSE	-	Remote Operations Service Element
SAFENET	-	Survivable Adaptable Fiber Optic Embedded Network
SDNS	-	Secure Data Network Systems
SG	-	Sub Group
SM	-	Security Management
SMF	-	Systems Management Function
SMFA	-	Specific Management Functional Area
SMI	-	Structure of Management Information
SMP	-	Simple Management Protocol
SNMP	-	Simple Network Management Protocol
SP3	-	Security Protocol 3
SP4	-	Security Protocol 4
SQL	-	Structured Query Language
STANAG	-	Standardization Agreement (NATO)
TCP/IP	-	Transmission Control Protocol/Internet Protocol
TELECOM	-	Telecommunications
TOP	-	Technical and Office Protocol
TP	-	Transaction Processing Protocol
TSGCE	-	Tri-Service Group on Communications and Electronics
UI	-	UNIX International
VT	-	Virtual Terminal
VOT NMS	-	Voice Oriented Telecommunications Network Management System
WAN	-	Wide Area Network
WG	-	Working Group
XMP	-	X/Open Management Protocol
XOM	-	X/Open OSI-Abstract-Data Manipulation

3.2 Definitions and/or explanatory information. The following definitions and explanatory information are applicable for the purpose of this handbook. In addition, terms used in this handbook and defined in the Glossary of Telecommunications Terms (FED-STD-1037) shall use the FED-STD-1037 definition unless otherwise noted. Relevant terms defined in FED-STD-1037 include: bridge; carrier sense, multiple access/collision detection (CSMA/CD); connection-oriented mode

transmission; connectionless mode transmission; data communication; fiber distributed data interface (FDDI); file transfer, access and management (FTAM); gateway; local area network (LAN); message handling systems (MHS); telecommunication; token-ring network; and wide area network (WAN).

3.2.1 Abstract Syntax Notation One (ASN.1). An abstract syntax can be thought of as a named group of types. ASN.1 is a flexible yet standard method of describing data structures for representation, encoding, transmission and decoding. ASN.1 provides a set of formal rules for describing the structure of objects independently of machine-specific encoding techniques.

3.2.2 Accounting management (AM). AM is one of the five major Systems Management Functional Areas (SMFAs) that is described in the ISO OSI Management Framework and System Management Overview standards. The AM SMFA defines requirements to enable identification or negotiation of mechanisms for associating and collecting system resource usage charges, to initiate or deactivate charging algorithms, and to monitor or to report account relevant information.

3.2.3 Association Control Service Element (ACSE). The ACSE provides essential services for applications related to connection establishment, connection termination, and connection aborting. One of the parameters used by ACSE to identify the particular application to which an association is to be established is the Application Entity (AE) title.

3.2.4 Attribute. An attribute is a property of a managed object and has a value. Mandatory initial values for attributes can be specified as part of the managed object class definition. Attributes are grouped into mandatory and conditional packages.

3.2.5 Cognizant Technical Official (CTO). The CTO is the person responsible for the technical requirements related to the source selection process. (*Federal Acquisition Regulation, Apr 1990*). If no CTO is appointed, the term "Acquisition Authority" should be used in this document.

3.2.6 Common management information services and common management information protocol (CMIS/CMIP). CMIS and CMIP are the services and protocol developed by ISO for OSI systems management. CMIP is the protocol used by an application process to exchange information and commands for the purpose of remotely managing computer and communication resources, while CMIS specifies the service interface to CMIP. CMIS/CMIP may be used over a variety of underlying protocol stacks, including full-stack OSI, a mixed upper layer OSI over TCP/IP, and just the IEEE lower layer stack (LLC and below). In the former case, in order to transfer management information between open systems using CMIS/CMIP, peer connections (associations) must be established. This transfer requires the establishment of an application association, a session connection, a transport connection, and, depending upon the underlying communications technology, network and link connections.

3.2.7 Configuration management (CM). CM is one of the five major SMFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The CM SMFA defines requirements to determine/monitor (via interrogation, polling or event-driven reporting), to detect changes in, and to control the arrangement, relationships, characteristics and state (for

example, initialize/terminate, activate/deactivate, idle/busy, etc.) of individual and specifiable aggregates of managed resources so as to maintain continuous operation and/or delivery of service. CM as used in this MIL-HDBK is not to be confused with CM as used in MIL-STD-483 (*Configuration Management Practices for Systems, Equipment, Munitions, and Computer Programs*) or MIL-STD-1456 (*Configuration Management Plan*).

3.2.8 Directory services. The Directory Services (IS 9594, CCITT X.500) is an application service which enables users to query on the names of other users (for example, message recipients, applications, hosts names) and to obtain additional network information (for example, originator/recipient addresses, application entity titles, Presentation Service Access Point (PSAP) of application entities, network address of host computers).

3.2.9 Domains. Domains represent different ways of aggregating and distributing management authority and/or management scope for any specific reason. Often, large, complex aggregations of resources are partitioned into domains to make the inherent complexity manageable. An illustrative domain partitioning is between telecommunications service providers and their service users. The provider domain consists of the provider-owned physical and logical resources that make up the provider's network. The user domain consists of the user-owned resources that comprise the user's private network. The services obtained from the provider domain may or may not be considered to be in the user's domain, while the resources that underlie these services are definitely not in the user's domain.

3.2.10 Element manager system. An element manager system manages the resources specific to a particular component class of a distributed system; for example, a bridge manager is an element manager system that manages LAN bridges.

3.2.11 Enterprise management. Enterprise management is the management of the aggregate of all systems and networks within an organization or enterprise.

3.2.12 Event. An event is any occurrence that changes the status of a managed object. The event may be spontaneous or planned, persistent or temporary, and may trigger other events or be triggered by other events.

3.2.13 Fault management (FM). FM is one of the five major SMFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The FM SMFA defines requirements to define, detect, identify, monitor, isolate the causes of, log, analyze, test for, trace and correct problems in abnormal or disabled managed resources.

3.2.14 Human engineering. Human engineering is the consistent presentation of management information from heterogeneous network resources (for example, help screens, summarized data, graphical user interfaces, ergonomics, etc.). The use of human engineering will enable the network manager to quickly and easily comprehend the NM system's capabilities, to use the NM functions efficiently, and to allow flexibility in performing the desired operations.

3.2.15 Managed object. Managed objects are abstract representations of resources in a network. A managed object may represent a physical entity, a network service, or an abstraction of a resource which exists independently of its use in management. Managed object definitions of OSI resources, a critical requirement for interoperable NM systems, are beginning to be standardized. IS 10165-4 contains a set of standard guidelines for the definition of managed objects. IS 10165-2 and a number of the ISO/IEC 10164 series of standards contain definitions of common management information that can be imported into definitions of managed objects. Due to the importance of managed object definitions, many standards groups, vendors and user consortia (for example, CCITT, the IEEE 802, the NMF and the OIW (Open Systems Environment Implementors Workshop) NM Special Interest Group) are defining managed objects. The DoD has been active in defining military-unique managed objects. Specifically, MIL-STD-2204, SAFENET, defines a number of managed objects which are used to support the synchronization of distributed clocks in a tactical shipboard local area network.

3.2.16 Managed system. Managed systems contain agent processes that act on behalf of, and therefore interact with, remote manager systems or managed resources. The agent processes interact directly with the managed objects that characterize the managed resources. A single object may represent one or many resources, and a single resource may be characterized by one or many objects (each providing different management views of the actual resource). Such managed systems are often embedded in the hardware and/or software of the resource to be managed.

3.2.17 Management gateways. Management gateways translate and map between different management communication protocols, services, and/or different styles of representing the management information associated with specific resources. Such differences typically arise between (a) manager systems, such as n-layer managers or element managers, and (b) manager systems that manage an entire system. Differences also arise between managers of entire, but different, systems, such as managers of different protocol stacks. Management gateways can be used to accommodate management of existing, legacy resources. Management gateways can also be used to accommodate management of other future resources.

3.2.18 Management information base (MIB). A MIB is a distributed repository of the management information that represents the resources being managed. Many types of MIBs exist.

3.2.19 Manager system. A manager system is the hardware and software entity which receives management inputs from local operators, receives management inputs (such as spontaneous management-related notifications) from agent processes in remote manager systems (or in remote managed systems) and/or initiates requests for management information from agents in remote manager systems or in remote managed systems. (Management communications with remote manager systems or managed systems may occur via a standard, general purpose management communications protocol, such as CMIP.) A manager system can make management decisions via supported management applications. A manager system can effect decisions and other management operations either locally on local managed objects or remotely to manager systems or to managed systems representing remote managed objects.

3.2.20 Network. A network is a connected set of switching and transmission communication components. The network includes all hardware and software communications components residing in such switching and transmission components, as well as in end-systems, such as computers, that are attached to the network.

3.2.21 Network administrator. A network administrator is the person responsible for operating a NM system.

3.2.22 Network Control Center (NCC). An NCC is the top-level DoD NM entity within a management domain. The NCC coordinates and controls NM functions within a domain and between domains.

3.2.23 Network management (NM). NM is the set of activities to bring up and establish networking resources, keep them operational, fine tune their operation, account for their usage, and support their protection from unauthorized use and tampering. Typically, the term is also used to refer to such management activities as well as a myriad of other management functions and activities, of greater or lesser scope, when any of such management functions and activities are applied to other kinds of manageable resources besides telecommunications (voice), messaging, video and computer communications networks. Such other management functions and activities may be associated with the early planning stages, growth and retirement of resources, as well as with daily operation and utilization. Such other resources may include general purpose information processing resources such as computers, their system software/peripherals, the distributed multimedia applications they host, or the aggregate of all such resources together with the networking resources used to interconnect them.

3.2.24 Network management system (NM system). An NM system is the aggregate of the operational and administrative mechanisms, protocols, procedures and tools to provide NM. The NM system may consist of manager systems, managed systems, and management gateways.

3.2.25 Network manager. A network manager is a specialized manager system (see above) used to manage networking resources.

3.2.26 N-layer manager. An n-layer manager is a manager that manages the resources specific to one layer of a stack of networking protocols. Such managers often do not use general purpose management communication protocols (for example, CMIP), services and management information. Rather, they often use mechanisms and/or services specific to the protocol layer being managed.

3.2.27 Package. A package is a term used in the definition of OSI managed objects. A package refers to a collection of attributes, notifications, operations, and/or behaviors which are treated as a single module in the specification of a managed object class. Packages may be specified as being mandatory or conditional when referenced in a managed object class definition. However, the provision of options in managed object class definitions is discouraged on the grounds that internetworking becomes more difficult as the number of conditional packages increases.

3.2.28 Performance management (PM). PM is one of the five major SMFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The PM SMFA defines requirements to provide the attributes, services, and event reports to measure, estimate, monitor (via interrogation, polling or event driven reporting), track, store, analyze/evaluate, maintain and otherwise control the configuration, operational characteristics, performance/effectiveness characteristics, performance measuring/monitoring characteristics, performance tuning characteristics, performance testing characteristics and/or quality-of-service characteristics and objectives (for example, responsiveness, availability, utilization, and residual capacity) associated with individual managed resources or specifiable aggregates of managed resources.

3.2.29 Remote Operations Service Element (ROSE) protocol. ROSE provides remote operation capabilities, allowing request/response interaction between entities of a distributed application. That is, upon receiving a remote operation request from one entity, the receiving entity attempts to perform the requested operation and reports the outcome of the attempt to the requesting entity.

3.2.30 Router. A router is a device that provides the network layer relay function connecting two subnetworks. That is, the device receives data from one network entity and forwards it to another network entity.

3.2.31 Security management (SM). SM is one of the five major SMFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The SM SMFA defines requirements to support combat of threats by identifying and logging users of sensitive resources, monitoring usage of sensitive resources, defining, identifying, and monitoring security-relevant events, creating, and analyzing audit trails of such events, users and usage, controlling certain aspects of security services and mechanisms (for example, initiating re-keying or algorithm re-initialization), and controlling configuration (for example, isolating infected resources or denying/limiting resource access to unauthorized applications, users, or their requests).

3.2.32 Specific management functional area (SMFA). ISO has partitioned systems management into five SMFAs to categorize requirements for the support of systems management. The five SMFAs are: configuration management, fault management, performance management, security management, and accounting management. System Management Function standards (see para 3.2.35) define management services/capabilities to meet these requirements. In some cases, different SMFAs have the same requirements and therefore use the same SMFs to satisfy the common requirements.

3.2.33 System. A system is a set of information processing and data processing resources (such as computers), together with any supporting system software (such as operating systems and DBMSs), any peripheral devices, any supported applications and files, and any communications infrastructure that interconnects the system's components, end-users of such system resources, and the users and components of other systems. A system is generally considered to include all hardware and software components, facilities, personnel, and procedures which are necessary to support applications.

3.2.34 Systems management. Systems management is the set of activities to bring up and establish system resources, keep them operational, fine tune their operation, account for their usage, and support their protection from unauthorized use and tampering. Typically, as with the term *network management*, the term *systems management* is also used to refer to a myriad of other management functions and activities, of greater or lesser scope, which may also be applied to the management of resources other than system resources.

3.2.35 Systems Management Function (SMF). The SMFs include functions such as object management, state management, alarm reporting, event report management, log control, security alarm reporting, and accounting meter. The many parts of ISO/IEC 10164, are the SMF standards that define specific services, notifications (events), and/or attributes to support different NM requirements.

4. GENERAL REQUIREMENTS

(NOTE: Tutorial information is indented.)

4.1 Overview. This section describes general requirements for DoD NM systems. Requirements for NM architecture, management applications, NM system characteristics, security for NM, and tactical systems management are covered.

Because these requirements are general in nature, the CTO should reference specific requirements from section 5 (Detailed Requirements) for acquisitions. Specific sections or sub-sections of section 5 should be cited when applicable for specific DoD acquisitions.

4.2 NM architecture. Using the specifications included in and referenced by this MIL-HDBK, three types of logical management components/services can be procured: managed systems, manager systems, and management gateways (also called proxy managers or proxy agents or mediation devices). Management gateways should be used to interface NM components/services that rely on disparate management communication protocols, disparate management services, disparate management information, or any other disparate NM tools, capabilities, or features.

These three types of management components/services may be combined, organized, interconnected, and used in a variety of CTO-specified ways. It should be possible to dynamically aggregate or re-aggregate such components/services into management domains, using arbitrary aggregation or reaggregation criteria. Domains themselves should be able to be organized and interconnected in a variety of ways, including hierarchical and peer-to-peer (see figure 1, page 23). These three types of management components/services should support CTO-specified capabilities for the following Systems Management Functional Areas (SMFAs): configuration management, fault management, performance management, accounting management, and security management.

As per GNMP, it should be possible to support the integration of multiple managers, multiple managed systems, and multiple management gateways so as to allow common observation and control of the composite of disparate logical and physical resources/services.

> Current approaches for managing the totality of resources within a domain are often fragmented. Resources within a domain are typically managed by a group of single-function manager systems. These manager systems are each focused on a small fraction of the resources within the domain; and, these manager systems do not work together. These manager systems are disjoint, both logically and geographically.

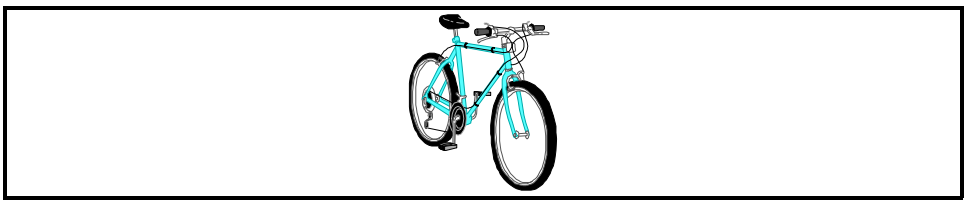

FIGURE 1. Abstract view of management domains.

It can be argued that the multiple-independent-managers concept makes development less complex because it does not require that a single manager system handle all possible variations of equipment. For example, telecommunications managers need not implement functions special to ISO 8802/5 token-ring networks and vice versa.

However, characteristic of most of today's multiple-independent-manager approaches, there is no common view of the composite of all resources within the domain. Information processing paths that involve heterogeneous classes of resources can not be readily traced for configuration and fault assessment. Related fault indications can not be readily correlated; accordingly, it is difficult to pin point root-cause failures from a myriad of symptoms often appearing concurrently in different classes of resources when a problem arises. It is difficult to assess the cost-effectiveness of the services delivered by or provided by the aggregate of the resources within the domain. It is also difficult to provide realistic strategic information pertinent to predicting what changes and additions will be required to the resources within a domain as the organization(s) using the services provided by the resources evolve(s).

To the maximum extent possible, the managed systems, manager systems, and management gateways components/services should support the conformance and interoperability requirements in section five of the GNMP. That is, the management protocols, functions, tools, and information used among such components/services should be in accordance with the GNMP. See section 1.9. Section 6.5 of this MIL-HDBK contains further considerations that may apply to the testing of components/services to be acquired.

4.2.1 Management information. As required by the CTO, DoD NM systems may be capable of supporting two types of management information pools: (1) databases (both integrated and non-integrated) and (2) MIBs. As a minimum, MIBs should be supported.

Databases are archival repositories persistently stored on electro/optical media. Databases are accessed/updated by database management systems. Databases ae generally used by, and shared among, manager systems by means of standard database query languages, such as SQL and RDA. Some databases may be integrated across several different manager systems and/or management domains.

MIBs are management information bases that are distributed repositories of the managed objects that represent the resources being managed. MIBs are also run-time, real-time repositories available to be shared among manager systems, managed systems, and management gateways by means of standard management communication protocols.

The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, should be specified by the CTO. Management system

components/services should have a common understanding of management information databases and MIBs, access characteristics, and the structure of managed objects.

To achieve such common views and knowledge, multi-acquisition coordination is likely to be required in situations where the management entities procured under one acquisition need to interact with the management entities procured under another acquisition.

To the maximum extent possible, management information specified in GNMP should be used for MIBs. If the required management information is not specified in GNMP, management information specified in the other sources of specifications in section 1.9 may be used. Any other management information required by the CTO may be defined as specified in section 5.2.5.5 and in accordance with rules stated in the GNMP. Management information identified in the management and security policies in effect at any given instant should be able to be accessed by, shared among, and/or modified by appropriate distributed management components/services.

4.2.2 Network control center (NCC). Overall management responsibility in a domain should be assigned to a logical NCC. An NCC should coordinate NM functions:

a. within its domain of jurisdiction; and

b. between its domain and other domains.

Accordingly, an NCC should have appropriate managed system, manager system, and management gateway capabilities to allow it to interact with, and pass appropriate management information and commands among, NM components/services in its own and other domains. An illustrative arrangement of NCC's associated with different domains organized hierarchically and in peer-to-peer fashion is portrayed in figure 2, page 26.

It should be noted that an NCC can be a single physical entity or it can be a logical entity distributed over several manager systems, each of which are typically within the domain of jurisdiction of the NCC.

The CTO should determine survivability requirements for the NCC and determine the NCC's availability to support devolution of control from:

a. NCC's in other domains; and

b. manager systems within its domain of jurisdiction.

By appropriate back-up, recovery, and/or shadowing principles, any NCC or any other manager system can serve as the hot backup for any other NCC. In fact, a sequence of hot backups can be put in place for extremely critical NCCs or for specific, extremely critical, NCC functionality.

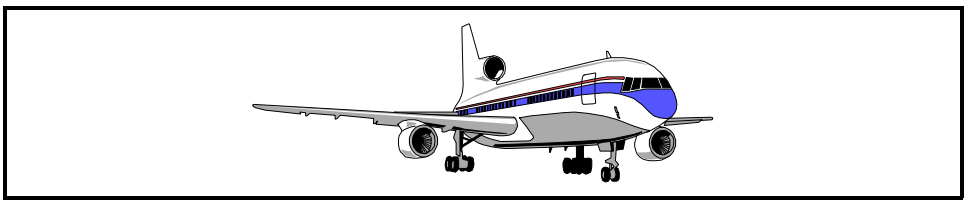

Figure 2. An Example Hierarchical Structure

To the maximum extent possible, a NCC should use the OSI systems management protocols, functions, services, and information specified in GNMP. If the GNMP does not provide the capabilities needed, the CTO may use the other sources of specifications identified in section 1.9 in order to provide needed capabilities.

4.3 Management applications. As required by the CTO, manager systems should be able to support the installation and execution of portable management applications across all management system platforms within the domain. Such applications should include one or more of at least the following applications:

a. management information development and maintenance tools;

b. integrated alarm reporting and trouble tracking;

c. disaster preparedness and recovery;

d. change and inventory control management; and

e. training aids.

As required by the CTO, management applications should be able to share their management information repositories and to support common management operations upon such repositories.

4.4 Management system characteristics. Sound human engineering (ergonomics) factors should be used throughout management system components/services to enable rapid, unambiguous comprehension and use of the capabilities provided. The CTO should specify the network analysis tools necessary to create several different types of pre-determined, pre-programmed and/or new, ad-hoc, on-demand information reports. These analysis tools should include mechanisms that enable the appropriate tool(s) and report(s) to be selected by the network administrator during live management operations.

The management system should meet all CTO-specified performance requirements, such as those pertaining to the network bandwidth consumed by NM traffic, processing speeds and capacities of management components/services, processing speeds, and capacities associated with management databases and MIBs, processing speeds and capacities associated with management displays, and the accuracy of management system analyses. The management system should support the ability for end-users of the resources and services being managed to interact with management system components/services in ways specified by the CTO. Refer to section 5.3 for specific details.

4.5 Security for management. As required by the CTO, management system components/services should:

a. support the security policy that is in effect with respect to the internal operation of management system components/services and with respect to interoperation among management system components/services; and

b. use CTO-specified security mechanisms to combat:

(1) modification of management information that is either resident within a management system component/service or in transit between management system components/services;

(2) unauthorized execution of management operations via masqueraded parties/entities;

(3) analysis of communications traffic among management system components/services for the purpose of inferring information about the systems being managed or about how to subvert the operations and/or management of the systems being managed; and

(4) denial of NM services.

As appropriate, the security provided for NM should be in accordance with draft MIL-STD 2045-38000. If other security is required or development of other security services/mechanisms is necessary, approval of the DAA (designated accreditation authority) may be required. The application for such approval should include a transition plan detailing the steps to be followed in migrating to COTS standards-based security.

4.6 Tactical systems management. The management requirements applicable to DoD management systems in general, i.e., the management requirements stipulated in this MIL-HDBK, also apply to the management of tactical system resources. In some situations, or as required by the CTO, the performance requirements associated with tactical systems management may be more rigid than with other DoD systems management, especially in areas such as:

a. conservation of bandwidth consumed by NM traffic;

b. ability to adapt dynamically to managing real-time, time-varying resource configurations;

c. ability to maintain NM control despite the high degree of intermittent interruptions in management communication services;

d. resumption of control of a failed NCC; and

e. other high survivability requirements.

5. DETAILED REQUIREMENTS

(NOTE: Tutorial information is indented)

5.1 Overview. This section describes detailed requirements for DoD NM systems. Requirements for NM architectures, NM system characteristics, OSI Systems Management Functional Areas (SMFAs), security for NM, and tactical systems management are covered. Cognizant Technical Officials (CTOs) should reference these requirements by section number of this MIL-HDBK whenever specific requirements of this MIL-HDBK apply to applicable DoD acquisitions. As indicated below, the applicability of a number of these requirements should be determined by each CTO. In these cases, the quantification of requirements into testable requirements for applicable procurement should be determined by each CTO.

CTOs are requested to provide feedback pertaining to this MIL-HDBK. In particular, CTOs are requested to send information regarding acquisition-specific applicability and quantification of the requirements herein to DISA/JIEO. Also, CTOs are requested to send information describing any additional acquisition-specific NM requirements to DISA/JIEO. Such feedback will be used to refine and to extend NM requirements that will be included in future versions of this MIL-HDBK. The point of contact for this MIL-HDBK is DISA/JIEO, Attn: TBD, 11440 Isaac Newton Square, Reston, VA 22090. (Note: *TBD* is an *office symbol* and is not to be confused with *to be determined*!)

5.2 NM architecture. Using the specifications included in and referenced by this MIL-HDBK, three styles of logical management components/services can be procured: managed systems, manager systems, and management gateways (also called proxy managers, proxy agents, and mediation devices).

The manager systems and managed systems should support the conformance requirements in the GNMP. The CTO should identify the specific conformance requirements for each such component/service being procured. Under extenuating circumstances, and as specifically required and identified by the CTO, such components/services may be based on other specifications identified in section 1.9. Since management gateways are not currently specified in the GNMP, CTOs should use other sources in section 1.9,such as those listed in section 2.2.3, as the basis for management gateway requirements and specifications.

These three types of management components/services, i.e., managed systems, manager systems, and management gateways, should be capable of being combined and used in a variety of ways, as described in this section, to form flexible NM architectures that can be tailored by CTOs to specific DoD procurement. Specific instances of NM architectures should be individually specified within each DoD procurement.

The remaining subsections of section 5.2 identify requirements of NM architectures. These include:

a. domains (section 5.2.1);

b. global Network Control Center (NCC) systems for domains, possible relationships among NCC components/services and other NM components/services, and management information available to/from NCCs (section 5.2.2);

c. management capabilities within, and management relationships among, management components/services within domains (section 5.2.3);

d. relationships among management components/services in different domains (section 5.2.4);

e. management information used by NM components/services (section 5.2.5); and

f. relationships among the above NM requirements and OSI systems management/GNMP (section 5.2.6).

5.2.1 Domains. As per the GNMP, the set of network (and eventually computing) resources to be managed should be capable of being partitioned into an acquisition-specific number of management domains. Allocations and reallocations of resources to domains, as well as managers to domains, should be capable of being made dynamically according to a variety of factors, including at least the following: ownership, mission, mission function, organization, geography, administration, accounting, technology, equipment or resource or resource service type being managed, performance requirements, management policy, and security policy.

The mechanisms and procedures to support such reallocation should be made publicly available so as to foster interoperability across acquisitions. Domains should be capable of being partitioned into a number of subordinate domains, each of which may have its own manager. Accordingly, as required by the CTO, a management domain should be able to accommodate more than one manager systems managing resources within the domain. Overall management responsibility in a domain should be capable of being assigned to a logical Network Control Center (see section 5.2.2).

Relationships must exist between domains established for management purposes and domains established for security purposes. Guidelines for such relationships appear in Appendix H.

5.2.2 Network Control Center (NCC). As directed by the CTO, an NCC should be capable of being used in each domain as a logically centralized management facility capable of coordinating NM functions within its domain of jurisdiction (see section 5.2.3), as well as among other domains (see section 5.2.4). A NCC should be able to coordinate with NCCs and managers in other domains to facilitate and manage a network and/or system service that utilizes resources across more than one domain. For example, a NCC should be able to provide integration of NM activities by allowing interoperation with other NCCs in strategic, sustaining base, and tactical networks.

It should be noted that an NCC can be a single physical entity or it can be a logical entity distributed over several manager systems, each of which are typically within the domain of jurisdiction of the NCC.

A NCC should use the OSI systems management protocols, functions, services, and information specified in the GNMP. A NCC should support the Systems Management Function (SMF) conformance requirements in the GNMP. If needed, a NCC should secondarily use any additional OSI-based specifications from the other sources of specifications (section 1.9), to support the following requirements:

a. agent capabilities (section 5.2.2.1);

b. manager capabilities (section 5.2.2.2);

c. management gateway capabilities (section 5.2.2.3);

d. management information (section 5.2.2.4); and

e. survivability and other requirements (section 5.2.2.5).

5.2.2.1 NCC agent capabilities. A NCC should support management agent capabilities. Subject to acquisition-specific management policies and security policies, when a NCC acts in the agent role, it should allow forwarding of management event reports, and/or responding to, management requests from acquisition-specific management entities including:

a. other NCCs;

b. lower-level managers and/or management gateways within its own domain of jurisdiction; and

c. lower-level managers and/or management gateways within other domains.

5.2.2.2 NCC manager capabilities. A NCC should support manager role capabilities, concurrently with the agent role capabilities. When a NCC acts in the manager role, subject to acquisition-specific management policies and security policies, it should be able to allow for monitoring (accepting event reports from) and controlling (sending management requests to) a variety of acquisition-specified management entities such as:

a. other NCCs;

b. lower-level managers and/or management gateways within its own domain of jurisdiction;

c. lower-level managers and/or management gateways within other domains;

d. managed systems in its own domain of jurisdiction; and

e. managed systems in other domains.

5.2.2.3 NCC management gateway capabilities. If needed by the CTO, a NCC should be able to function as a management gateway. The CTO should specify the disparate management protocols, services, functions, and/or management information that are to be interfaced by means of the NCC management gateway. For gateways between Internet and OSI management paradigms, the CTO should reference the specifications in section 2.2.3. These ISO/Internet Management Coexistence specifications provide mappings between Internet communication protocols (SNMP and SNMP v2) and OSI management communication protocols as well as mappings between OSI SMI and Internet SMI, as well as translations of certain MIBs. Other MIBs are likely to be translate, registered, and catalogued by the NMF or the OIW NM Special Interest Group.

5.2.2.4 NCC management information. A NCC should be able to provide the following types of management information to other NCCs, managers, and/or management gateways:

a. summary management information and/or significant summary event reports to other NCCs, such as neighboring (peer) NCCs and NCCs of any hierarchically, higher-level management domain;

b. detailed management information and/or significant summary event reports about its own domain to other NCCs, or to managers and/or management gateways within its domain of jurisdiction; and

c. management policy and security policy information from hierarchically, higher-level NCCs to neighboring (peer) NCCs, to NCCs of any hierarchically, lower-level management domain, and to managers or management gateways within its domain of jurisdiction.

The pairings of NM components among which management information is authorized to be passed, the specific management information elements that are authorized to be passed, and any further constraints on the passing of each specific element of management information, should be as identified in the management and security policies in effect within a domain, or across domains.

The precise management information to be passed to and/or from an NCC needs to be identified by the CTO. As needed for an acquisition, management information specified in the GNMP should be used. If not specified in the GNMP, management information specified in the other sources of specifications (section 1.9) should also be used. Any other management information required by the CTO should be defined in accordance with rules stated in the GNMP.

As needed by the CTO, registration services for management information definitions should be provided in accordance with section 5.2.5.5.

5.2.2.5 NCC survivability and other requirements. To support survivability requirements, and/or to support potential new management policies arising out of specific situations, such as during war time or during joint maneuvers, it should be possible, subject to any operational and/or security policies, for

an NCC in one domain to *cut through,* monitor, and directly control another domain. This *cut through* would be done without any intervening managers or NCCs, specific resources in its own domain, or specific resources in other domains.

To support survivability, availability, and devolution of control requirements, especially in times of emergency, it should also be possible for a hot backup to take over for an incapacitated NCC, subject to performance requirements as identified in section 5.3.4.2.

> Hot backups are fully configured sites which can take over all the functions of the primary site they are backing up. They are set up to come on-line within a short time after the primary site fails. By appropriate back-up, recovery and/or shadowing principles, any NCC or any other manager system can serve as the hot backup for any other NCC. In fact, a sequence of hot backups can be put in place for extremely critical NCCs or for specific, extremely critical, NCC functionality.

The precise survivability, availability, and devolution of control requirements and procedures should be specified by the CTO, in coordination with the CTOs or network administrators responsible for other NCCs that are expected to be included as part of the back-up and recovery strategy. The mechanisms and procedures used by a specific acquisition to support such requirements should be made publicly available so as to foster interoperability across acquisitions.

5.2.3 Management capabilities and relationships within domains. The management capabilities within domains should be as indicated in section 5.2.3.1. The relationships among management components/services within a domain should be as indicated in section 5.2.3.2.

5.2.3.1 Management capabilities within domains. As required and as specified by the domain-specific CTO and as approved by the Executive Agent, the management components/services that should be included within a management domain are manager systems, managed systems, and management gateways. The precise manager capabilities, agent capabilities, SMFs supported, and/or management information supported by each component/service within a domain should be identified by the CTO.

The types of management information that can be used within domains and passed among NM components within a domain should be specified by the CTO. As needed for an acquisition, management information specified in the GNMP should be used. If not specified in the GNMP, management information specified in the other sources of specifications (section 1.9) should also be used. Any other management information required by the CTO should be defined in accordance with rules stated in the GNMP. Management information used within a domain should also meet the requirements stipulated in section 5.2.5.

As needed by the CTO, registration services for management information definitions will be provided in accordance with section 5.2.5.5. The CTO should also specify the disparate management protocols, services, functions and/or management information that are to be interfaced by means of all

management gateways that are to be procured for use within the domain. For gateways between Internet and OSI management paradigms, see the guidance in section 5.2.2.3.

As required by the CTO, the coordinated and integrated management capabilities across the domain should support a variety of SMFA capabilities as indicated in section 5.4.
Support of legacy management systems should be done on a very limited basis as required by economic and/or mission needs. Additional consideration must be given to transition to fully interoperable systems as per section 1.9.1.

As required by the CTO, these capabilities should support the distributed installation and execution of portable management applications across all management system platforms within the domain. As required by the CTO, such management applications should share their management information bases (MIBs) and their databases; and they should support common management operations upon their MIBs and databases. Accordingly, management applications must support the ability to integrate, and/or transition among, heterogeneous styles of management for managing heterogeneous classes of resources.

> The goal of providing coordinated and integrated management across the domain is to allow common observation and control of the composite of any and all of the logical and physical resources within the domain.

5.2.3.2 Management relationships within domains. As per the GNMP, the integration of multiple manager systems, multiple managed systems and multiple management gateways should be supported within domains. As required by the CTO, coordinated and integrated management of any pairing of manager systems/NM components may be arranged in hierarchical and/or peer-to-peer fashion among manager systems within the domain. Similar hierarchical or peer-to-peer relationships may exist among any pair of the following NM components within a domain: manager system, managed systems, and management gateways depending upon management and security policies in effect.

The pairings of NM components among which management information is authorized to be passed within a domain, the specific management information elements that are authorized to be passed between each such pair, and any further constraints on the passing of each specific element of management information should be as identified in the management and security policies in effect within the domain.

> Figure 3, on page 37, shows an exemplar domain supporting the integrated management of backbone network transmission services provided by a combination of data communication transmission services and telecommunication transmission services within an organization. The domain pictured consists of two subordinate domains, each of which may have its own manager system. Figure 4, page 39 is a specific example of a NM implementation based on figure 3, page 37.

The telecommunications transmission services management domain includes resources that provide connectivity for circuit switching, message switching, and packet switching among users via a switch complex. The NM architecture includes, for example, management interfaces to PBXs, DPASs, channel banks, multiplexers, and mobile tactical systems. A migration to ISDN is anticipated.

The data communications transmission services management domain typically is a collection of LAN and WAN resources providing packet-switched connectivity among host computers, workstations, and terminals. The current, diverse systems in this category, often with proprietary protocols, will also undergo an evolution to standard implementations. In the future, the telecommunications and data communications management domains are expected to be merged.

As may be required by the CTO, the domain portrayed in Figure 3, page 37 may include other subordinate domains, for example, subordinate domains which contain base or tactical interfaces to the long-haul communications facilities. Subordinate domains should include the gateways to DDN (DISN) and DSN military networks, the gateways to the common carriers, and the services offered by such long-haul networks, all of which may have their own management facilities.

As per the GNMP, the DoD should require that OSI systems management protocols, functions, services, and management information representations be used between open manager systems and (see figure 3, page 37):

a. OSI managed systems;

b. OSI management gateways;

c. open element managers; and

d. open layer manager systems.

Otherwise, DoD should require that management protocols, functions, services, and management information representations from the other sources of specifications identified in section 1.9 be used for all other management interactions within a domain, namely for interactions between (see figure 3, page 37):

e. OSI management gateways and open (non-OSI) manager systems;

f. OSI management gateways and legacy, proprietary managed systems;

g. OSI management gateways and proprietary element managers;

h. open element managers and open (non-OSI) managed systems; and

i. open layer manager systems and the OSI and non-OSI layer systems they manage.

The management protocols, functions, services, and information used among OSI management gateways should be in accordance with the GNMP or any of the other sources of specifications identified in section 1.9.

FIGURE 3. Illustrative Interdomain Management Architecture

5.2.4 Management relationships among domains. A NCC shall be capable of being exposed to direct interconnection with NCCs and NM components in other domains. As specified by the CTO, specific manager systems, managed systems, and management gateways may be exposed to direct interconnection with NCCs in other domains. The relationships between a NCC in one domain, and a NCC or other NM components in another domain, should be as indicated in section 5.2.2.1.

As required by the CTO, a DoD NCC should be able to internetwork with the NATO NCC. The NATO NCC is the top-level manager system for all NATO resources. It internetworks with the NCCs of member nations. Each member nation's NCC coordinates the management of the member nations's networking resources/services. (See additional tutorial in Appendix F.)

The types of management information that can be passed among domains should be specified by the CTO. As needed for an acquisition, management information specified in the GNMP should be used. If not specified in the GNMP, management information specified in other sources of specifications (section 1.9) should be used. Any other management information required by the CTO should be defined in accordance with rules stated in the GNMP.

As needed by the CTO, registration services for management information definitions should be provided in accordance with section 5.2.5.5.

> Examples of management information shared between domains include: (a) reports of types of networking services offered by resources within a domain; (b) reports of the quality-of-service limits, for example delay, throughput, reserve capacity, security levels available, fault-tolerance, priorities available, etc., currently available via networking services offered by resources in a domain; (c) requests for use and/or reservation of specific networking services, with specific performance characteristics, that can be made available by resources within a domain; and (d) requests for configuration, performance history, and/or fault history information about resources and/or services available within a domain.

The pairings of NM components among which management information is authorized to be passed between domains, the specific management information elements that are authorized to be passed, and any further constraints on the passing of each specific element of management information between domains should be as identified in the management and security policies in effect across the domains. The specific elements of management information that are to be generally available, without any distribution control constraints to NM components outside a domain, should be made publicly available to facilitate management interoperability across domains procured under the jurisdictions of different CTOs. Further requirements on management information are as indicated in section 5.2.5.

As required by the CTO, management domains shall be capable of supporting two types of domain interaction paths: hierarchical, (see section 5.2.4.1), and peer-to-peer management relationships (see section 5.2.4.2).

FIGURE 4. An example NM system implementation

5.2.4.1 Hierarchical tree relationships among domains. It should be possible to support management interactions across several logically vertical levels of management domains. The number of such levels is to be specified by the CTO.

The concept of hierarchical management domains is necessary to manage the size and complexity of the total DoD network environment, which itself is often organized hierarchically to match the DoD's command structure. Delegation of management authority among domains avoids scaling problems associated with centralized management, but allows for distribution and enforcement of high-level DoD management and security policies from a central authority.

In hierarchies, it is typical for domain managers to have increasing degrees of specialization from the top to the bottom of the hierarchy. Accordingly, some managers will be specialized to manage only one type of resource, whereas higher-level managers will coordinate the roles of those at lower levels. The actual number of levels of the management hierarchy can vary as a function of the complexity of the portion of the DoD network being managed.

As per the DISN Goal Integrated Communications Architecture and Transition Strategy, the entire DISN management domain structure consists of (a) a top-level global, inter-theater NCC; (b) regional-level theater-specific (for example CONUS, European, Pacific), area NCCs; (c) metropolitan, inter-base NCCs; (d) base-level NCCs; possibly (e) local, intra-base NCCS; and (f) special-purpose NCCs.

Figure 5, page 41 depicts an exemplar set of hierarchical relationships among NCCs.

5.2.4.2 Peer-to-peer relationships among domains. It should be possible to support management interactions across several logical peer management domains. The number of such peer relationships is to be specified by the CTO. Peer-to-peer relationships should be able to exist at different hierarchical domain levels, as identified by the relevant management and security policies in effect.

The following example typifies a certain type of peer-to-peer relationship, where resources owned by one domain are managed by another. Telecommunications service users may have a user domain manager that also manages some aspects of the provider equipment that resides at the user's premises; or, in contrast, the service provider could offer a comprehensive management service that includes management of customer-owned resources.

Figure 5, page 41 also illustrates exemplar peer-to-peer management interaction paths among domains.